MAYER BROWN LLP
Lauren R. Goldman (*pro hac vice*)
Michael Rayfield (*pro hac vice*)
1221 Avenue of the Americas
New York, NY 10016
(212) 506-2500
lrgoldman@mayerbrown.com
mrayfield@mayerbrown.com

Matthew D. Provance (*pro hac vice*)
71 Wacker Drive
Chicago, IL 60606
(312) 701-8598
mprovance@mayerbrown.com

COOLEY LLP
Michael G. Rhodes (116127)
Whitty Somvichian (194463)
101 California Street, 5th Floor
San Francisco, CA 94111
(415) 693-2000
rhodesmg@cooley.com
wsomvichian@cooley.com

Attorneys for Defendant Facebook, Inc.

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

**SAN FRANCISCO DIVISION**

CLAYTON P. ZELLMER,

Plaintiff,

vs.

FACEBOOK, INC.,

Defendant.

Case No. 3:18-cv-1880-JD

**DEFENDANT'S MOTION FOR SUMMARY JUDGMENT**

Date: July 8, 2021
Time: 10:00 a.m.
Location: Courtroom 11, 19th Floor
Judge: Hon. James Donato
Trial Date: April 11, 2022
Complaint Filed: March 27, 2018

[*Declaration of Gary McCoy and proposed order filed concurrently*]

## NOTICE OF MOTION & MOTION

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE THAT, on July 8, 2021, at 10:00 a.m., before the Honorable James Donato, defendant Facebook, Inc. will and hereby does move for summary judgment on each of plaintiff's claims under Federal Rule of Civil Procedure 56. Facebook requests oral argument.

## STATEMENT OF RELIEF SOUGHT

Facebook seeks summary judgment on each of plaintiff's claims or, alternatively, on plaintiff's claim for injunctive relief.

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Cases**

**Statutes**

**Other Authorities**

## INTRODUCTION

Clayton Zellmer has never used Facebook. Until he filed his suit, Facebook had never interacted with him; it had no means of interacting with him; and it had no idea who he was. But Mr. Zellmer claims that he appeared in photographs uploaded to Facebook by other people, and that Facebook violated the Illinois Biometric Information Privacy Act ("BIPA") by applying facial-recognition technology to those photos without giving him notice or obtaining his consent. Any data generated from photos of Mr. Zellmer was not—and could not be—used to identify him, and that data was discarded nearly the instant it was created. There is no way for Facebook to give notice to, or obtain consent from, non-users like Mr. Zellmer who merely appear in uploaded photos. So Mr. Zellmer's claim is, at bottom, that Facebook should not be using facial recognition at all, even though Facebook users affirmatively consent to the feature and can opt out at any time.

As this Court explained in another case brought on this theory, that is "more than Illinois contemplated" when it enacted BIPA. In *Gullen v. Facebook*, a non-user case dismissed in 2018 on unrelated grounds, the Court pressed Mr. Gullen's counsel (now Mr. Zellmer's counsel) on a simple question: how can a "written notification and consent statute [ ] apply to people who are non-users?" The Court found it "patently unreasonable" to require Facebook to "proactively get the written consent of anybody who might show up in a Facebook photograph"; that is not "what the BIPA was supposed to address." Plaintiff's counsel never offered a meaningful answer.

Five years after the *Gullen* action was filed, Mr. Zellmer's counsel still has no answer. The Court should grant summary judgment in favor of Facebook for three independent reasons.

First, any data Facebook derives from images of non-users cannot be used to identify those individuals. This data is therefore unregulated by BIPA: BIPA covers only "biometric identifiers" and "biometric information." 740 ILCS 14/15. As its name suggests, "the phrase 'biometric identifier' is commonly understood to refer to the measurement and analysis of a unique physical or behavioral characteristic that identifies a person." State of Illinois, Office of the Attorney General, Public Access Op. No. 17-011, 2017 WL 10084298, at *3 (Ill. A.G. Aug. 14, 2017) ("Ill. AG Op."). Similarly, BIPA defines "biometric information" as data "based on an individual's biometric identifier" that is "used to identify an individual." 740 ILCS 14/10. BIPA's legislative findings confirm that the statute is about "unique identifiers" that "are biologically unique to the individual" and therefore susceptible to "identity theft" if compromised. *Id.* 14/5(c). Neither Facebook nor anyone else could use data generated from photos of Mr. Zellmer to identify him.

Second, and relatedly, Facebook immediately discards any face-recognition data generated from photos of non-users like Mr. Zellmer, meaning that it is never "in possession" of such data (740 ILCS 15(a)) and does not "collect, capture, purchase, receive through trade, or otherwise obtain" it (*id.* 15(b)). Courts have routinely held that each of these statutory terms connotes an exercise of "dominion or control over [the] biometric data." *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 968 (N.D. Ill. 2020) (citing *People v. Ward*, 215 Ill. 2d 317, 325 (2005)). That is no surprise, because the mere creation of biometric data, without retention, does not raise the identity-theft concerns that the legislature had in mind. Facebook has relinquished the ability to "control" the face-recognition data generated from images of non-users like Mr. Zellmer.

Third, it would be impossible for Facebook to give notice to, or obtain consent from, non-users who appear in uploaded photos; again, Facebook has no relationship with them or any way of knowing who they are. Illinois courts have long refused to read statutes to require something that is "utterly impossible." *McDonald v. City of Spring Valley*, 285 Ill. 52, 56 (1918). BIPA should be no exception: The statute was intended to *regulate* the collection and storage of biometric data, not to preclude it. *See* 740 ILCS 14/5(a), (e), (g). As this Court has explained, and as Mr. Zellmer admitted at his deposition, his reading would amount to a "ban on the program." Indeed, it would require a ban on *most* prevalent applications of biometric technology, including the type of security applications that the Illinois legislature wanted to encourage. The Court should not construe a *notice and consent* statute to flatly preclude the use of a technology.

Facebook is entitled to summary judgment on each of Mr. Zellmer's claims. But if the Court disagrees, it should at least grant summary judgment on his claim for injunctive relief. An injunction is proper only if it would benefit all the people affected by it. Mr. Zellmer's proposed injunction would affect not only non-users who have no qualms with facial recognition, but also many people who use Facebook and enjoy the feature. Facebook's motion should be granted.

## BACKGROUND[1]

### A. The Illinois Biometric Information Privacy Act

BIPA was enacted in 2008 to address the growing use of biometric data "in the business and security screening sectors" in Illinois. 740 ILCS 14/5(a). The Illinois General Assembly found that "[t]he use of biometrics is growing in [these] sectors and appears to promise streamlined financial transactions and security screenings" (*id.*), including purchases powered by "finger-scan technologies at grocery stores, gas stations, and school cafeterias" (*id.* 14/5(b)). But because there is a "heightened risk for identity theft" when biometric data is "compromised" (*id.* 14/5(c)), "many members of the public [had been] deterred from partaking in biometric identifier-facilitated transactions" (*id.* 14/5(e)). The legislature found that the public would "be served by regulating" this data under certain circumstances. *Id.* 14/5(g).

BIPA regulates the collection and storage of (1) "biometric identifiers" and (2) "biometric information." *Id.* 14/10. The definition of "biometric identifier" covers six sources of data: "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." *Id.* Other potential identifiers, including "photographs," "demographic data," and "physical descriptions," are excluded from the definition. *Id.* The definition of "biometric information" includes "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual," and excludes "information derived from items or procedures excluded under the definition of biometric identifiers." *Id.*

Private entities that collect biometric data must comply with two requirements at issue here: First, an entity "in possession of" biometric data must publish and adhere to guidelines for the retention and destruction of the data. *Id.* 14/15(a). Second, before an entity may "collect, capture, purchase, receive through trade, or otherwise obtain" a person's biometric data, it must (a) inform the person "in writing" of the "specific purpose and length of term" for which biometric data is being "collected, stored, and used"; and (b) obtain a "written release" from that person, defined as "informed written consent." *Id.* 14/10, 14/15(b). BIPA also contains provisions about

[1] All cited exhibits are attached to the Declaration of Matthew D. Provance.

the sale and dissemination of biometric data to third parties (*id.* 14/15(c)-(e)), but Mr. Zellmer does not invoke those provisions.

BIPA provides a private right of action to any "person aggrieved by a violation of this Act." *Id.* 14/20. A plaintiff may recover the greater of "$1,000 or actual damages" against an entity that "negligently" violates a provision of BIPA, or the greater of "$5,000 or actual damages" against an entity that "intentionally or recklessly" violates the Act. *Id.* 14/20.

### B. Facebook's Facial-Recognition Technology

Facebook allows people around the world to connect and share content online, including photos, with one another. Compl. (Dkt. 1) ¶ 21. For many years, Facebook has made the sharing of photos more personal and social by allowing users to "tag" their Facebook friends. *Id.* ¶ 6. A tag consists of the person's name and a link to his or her profile.[2]

In 2011, Facebook launched a feature called Tag Suggestions that uses facial-recognition technology to make tagging easier for people who use Facebook. Generally speaking, when a person uploads a photo to Facebook, Facebook will sometimes attempt to determine whether the photo includes images of any of the uploader's Facebook friends who have the feature enabled. If there is a match, Facebook may suggest that the uploader tag those friends (which the user can accept or ignore). Facebook does not—and cannot—suggest tags for non-users. Taigman Dep. (Ex. 2) at 369; McCoy Dep. (Ex. 3) at 156.[3]

The details of Facebook's facial-recognition process, and how it works specifically for non-users, are described below. This description is based largely on the testimony of Yaniv Taigman and Omry Yadan, Facebook engineers who were instrumental to the development of its facial-recognition technology. Taigman Dep. at 26-27, 38, 100-01; Yadan Dep. (Ex. 4) at 20, 51. Mr. Taigman and Mr. Yadan were each deposed in *Gullen*. Gary McCoy, a Facebook engineer,

[2] Facebook users can also "tag" a non-user in an uploaded photo by manually entering the non-user's name or any random text; these tags do not contain links (because non-users do not have profiles), and consist only of whatever text the user enters. Mr. Zellmer was not tagged in any photo on Facebook. Zellmer Dep. (Ex. 1) at 71-74.

[3] A user can opt out of Tag Suggestions at any time. If a user opts out, Facebook will delete any facial-recognition information previously associated with that user, and the user's name will no longer be suggested.

has submitted a declaration describing the technology. McCoy Decl. (attached to this motion). At his deposition, Mr. McCoy confirmed that Facebook's technology works the same way in all relevant respects as it did when discovery in *Gullen* closed. McCoy Dep. at 55, 127-28.

### 1. Facebook's Four-Step Facial-Recognition "Pipeline"

When Facebook applies facial recognition to a photo, the process has four steps: detection, alignment, representation, and classification. McCoy Decl. ¶ 2.

***Detection.*** First, Facebook's software analyzes an array of pixels in a photo to determine whether *any* human faces are present. *Id.* ¶¶ 2-3. If a face is detected, the software produces a cropped image of the face (a "face crop") in a rectangular box. *Id.* ¶ 3. The face-detection process does not identify people who appear in the image; it determines only whether one or more faces are present, and the size and location of any faces. *Id.*; *see* Taigman Dep. at 126-27, 130-33, 137-40, 171; Yadan Dep. at 98-99, 117-18.

***Alignment.*** If a face is detected, the software locates a set of "fiducial points"—reference points on the image—that are used to "align" it by centering it, orienting it forward, and scaling it in size. McCoy Decl. ¶ 3; Taigman Dep. at 150-53, 159-67, 177-78. The fiducial points help "warp" and normalize the image. McCoy Decl. ¶ 5; Taigman Dep. at 366-67. The only data passed to the next step is the pixel array of the standardized image, not the fiducial points. McCoy Decl. ¶ 5; McCoy Dep. at 85-86; Taigman Dep. at 172.

***Representation.*** Facebook then analyzes the aligned face crop to compute a numerical "face signature"—a string of numbers that represents a particular image of a face. McCoy Decl. ¶ 7; Taigman Dep. at 171-72; Yadan Dep. at 156. These numbers do not reveal any geometric information about the face in the image. McCoy Decl. ¶ 7. Nor do they correspond to specific facial components like the eyes or nose, or distances between those components. *Id.* Nor could they be reverse-engineered to *derive* such measurements—the face signatures are simply abstract, numerical representations computed based on the millions of parameters of Facebook's specific network. *Id.* They are useless without that network. *Id.* And face signatures are *not* saved or stored; once they are used for the next step, they are discarded. *Id.* ¶ 8; McCoy Dep. at 40-41; Taigman Dep. at 237, 240-41, 340-41.[4]

***Classification.*** Finally, Facebook attempts to identify the face by comparing the newly created face signature with the stored "templates" of a subset of people on Facebook connected to the user who uploaded the photo. McCoy Decl. ¶ 9; Taigman Dep. at 273-74. A template is computed by a mathematical function that sorts data into two classes separated by a plane, known as a "hyperplane." McCoy Decl. ¶ 9. A particular user's face template is a hyperplane that divides two sets of face signatures: those that correspond to that user and those that do not. *Id.* If the comparison indicates a likelihood that the new face signature belongs to a particular friend of the uploader, Facebook may offer the uploader the chance to tag that friend; the friend can then either accept or reject the tag suggestion. *Id.* ¶ 10; Taigman Dep. at 273.

### 2. The Process For Photos Of Non-Users

When a photo uploaded to Facebook contains the face of someone, like Mr. Zellmer, who does *not* have a Facebook account, there are several key distinctions in how the process works.

Facebook does not create, save, or store templates for non-users who appear in photos. McCoy Decl. ¶ 13; McCoy Dep. at 39-40; Taigman Dep. at 369. As a result, the face signatures derived from images of non-users like Mr. Zellmer cannot be—and are not—used to *identify* anyone. *See* McCoy Decl. ¶¶ 15-16; Taigman Dep. at 368. When a user uploads a photo with a non-user's face, and the initial steps of the pipeline are successfully performed, Facebook's software calculates a face signature for that image and compares it to the templates of a subset of users connected to the uploader. McCoy Decl. ¶ 7. But because there will never be a match to a non-user, the face signature is immediately discarded. *Id.* ¶¶ 8, 11, 16; McCoy Dep. at 154-55; Taigman Dep. at 368. When a non-user face signature is created and analyzed for matches, the process turns up nothing unless there is an error. *See* McCoy Decl. ¶ 15; McCoy Dep. at 155-56.[5]

[4] For a variety of reasons—including failures of detection and alignment—the face signature "is not always returned or computed." Yadan Dep. at 156-57.

[5] On rare occasions, Facebook's system erroneously matches a non-user's face to a *user's* profile, but no *correct* match will ever be made for non-users. *See* Taigman Dep. at 369; McCoy Dep. at 44-45.

For these reasons, it is impossible for Facebook to provide non-users with notice or obtain their consent before creating a face signature from photos of their faces. To do so, paradoxically, Facebook would need to *identify* the non-user *before* subjecting the photo to facial recognition—which, again, Facebook cannot do. Nor is there any way for Facebook to exempt non-users from the two initial stages of the facial-recognition pipeline while still performing those processes on users. Facebook cannot determine whether someone in a photo is a non-user until the end of the process, after potential faces have been located and aligned and a face signature has been computed. McCoy Decl. ¶¶ 9-10, 14. To avoid using facial-recognition technology on non-user photos, Facebook would have to stop using the technology entirely.

### C. The *Gullen* Action

Mr. Zellmer's case is an offshoot of *Gullen v. Facebook, Inc.*, No. 16-cv-00937 (N.D. Cal.), a non-user BIPA action filed by the lawyers who represent Mr. Zellmer. The *Gullen* action was dismissed in 2018 on grounds that were specific to Mr. Gullen's case. But the Court's statements throughout the litigation have guided Facebook's selection of the issues to raise here. From the outset, the Court expressed skepticism that non-users could bring claims under BIPA, recognizing that there is no feasible way for Facebook to give them notice or obtain their consent.

At a hearing in June 2016, for example, the Court questioned Mr. Gullen's counsel at length on these issues, and received no satisfactory response:

> THE COURT: How would the BIPA work? I mean, ***BIPA is a written consent statute***. . . . Surely, you're not contending that under the BIPA, Facebook has to . . . proactively get the written consent of anybody who might show up in a Facebook photograph? I mean, ***that would be patently unreasonable. So I . . . don't understand how a . . . written notification and consent statute can apply to people who are non-users***. . . . How could [Facebook] comply with BIPA short of requiring . . . every living human in the state of Illinois to give proactive written consent? I mean, could it otherwise comply with BIPA?
>
> MR. HEDIN: It could disable the face scanning feature from all photographs uploaded from IP addresses . . . that correspond to the state of Illinois.
>
> THE COURT: In other words, just a ban in the program?
>
> MR. HEDIN: Possibly.
>
> THE COURT: So basically, in your view, BIPA would make it entirely illegal to do tagging? . . . . ***You're saying that BIPA would make it patently illegal with no exceptions to do tagging*** . . . .

Ex. 5 at 9-10 (emphases added).

On November 30, 2017, the Court had a similar exchange with a different lawyer representing Mr. Gullen. This time, Mr. Gullen's counsel did not go so far as to propose a ban on facial recognition, but his proposal was equally infeasible:

> THE COURT: ***[H]ow is Facebook supposed to reach [a non-user]? . . . Facebook can't alert 310 million Americans . . . . What are they supposed to do?*** . . . [S]uppose you're an Illinois family at the Grand Canyon and you take the rim crater shot and you do what everybody in my family does, you immediately upload it on site. How are they supposed to know?
>
> MR. MILIAN: ***That may not be a violation.***
>
> THE COURT: Where are you going to draw the line?
>
> MR. MILIAN: I think you draw the line with photos uploaded from the State of Illinois. . . .
>
> THE COURT: Facebook . . . gets millions of photographs a day, probably an hour. They are supposed to screen every photograph[?] . . . If I were in your position, I would begin thinking about how you're going to explain to me how this is supposed to work out. . . . I mean, you know, if I drive through Chicago and somebody [ ] takes a picture of me and it gets tagged on Facebook, ***I don't think that's what the BIPA was supposed to address.*** . . . I'm not a Facebook user. ***So it just seems more than Illinois contemplated.***

Ex. 6 at 31-34 (emphases added).

The Court ultimately did not reach these issues in *Gullen*, because it granted summary judgment to Facebook on a different ground: Discovery demonstrated that "Facebook did not use its facial recognition technology" on the only photograph of Mr. Gullen that had been uploaded from Illinois, and in response to a question from the Court, Mr. Gullen's counsel conceded that he could not bring a claim based on photos uploaded from other states. *Gullen v. Facebook, Inc.*, 2018 WL 1609337, at *1 (N.D. Cal. Apr. 3, 2018). The Ninth Circuit affirmed. *Gullen v. Facebook, Inc.*, 772 F. App'x 481, 482 (9th Cir. 2019).

### D. Mr. Zellmer's Claims

Mr. Zellmer first tried to assert his claims in the *Gullen* action. On January 19, 2018—about a month after Facebook moved for summary judgment—Mr. Gullen moved to amend his complaint "to protect the putative non-user class" by adding Mr. Zellmer. *Gullen* Dkt. 129 at 7. Meanwhile, Mr. Zellmer—still represented by the same counsel as Mr. Gullen—filed his own complaint against Facebook on March 27, 2018. Compl. (Dkt. 1). The district court denied Mr. Gullen's motion to amend, describing the motion as an untimely attempt to "shore up [the] deficiencies in Gullen's individual claims." *Gullen* Dkt. 143 at 1. After the Court granted summary judgment in *Gullen*, it stayed Mr. Zellmer's action pending the appeal in *Gullen* and in the related case brought by Facebook users (which has since settled). Dkt. 33; *see In re Facebook Biometric Info. Privacy Litig.*, No. 15-cv-3747 (N.D. Cal.). The Court lifted the stay on March 26, 2020. Dkt. 42. Fact discovery closed on April 26, 2021.

Mr. Zellmer alleges that he is "a resident and citizen of Illinois" and "has never been[] a Facebook user." Compl. ¶ 8. He claims that Facebook users uploaded five photos of him from Illinois. *Id.* ¶¶ 29-34. And he asserts that, without notifying him or obtaining his written consent (*id.* ¶ 39), Facebook "automatically scanned and analyzed Plaintiff Zellmer's face," "extracted his biometric identifiers," "used those biometric identifiers to create a digitized template of his face," and "then prompted [the uploader] to match a name to Plaintiff Zellmer's face" (*id.* ¶¶ 35-36). Similar allegations appear throughout Mr. Zellmer's complaint. *See, e.g.*, *id.* ¶ 22 ("Facebook's proprietary facial-recognition technology scans every user-uploaded photo for faces, extracts geometric data relating to the unique points and contours of each face, and then uses that data to create and store a template of each face."); *id.* ¶ 24 ("when a Facebook user uploads a new photo, Facebook's sophisticated facial-recognition technology creates a scan of a face geometry template for each face depicted therein, without consideration for whether a particular face belongs to a Facebook user or unwitting non-user," and "compares each template against Facebook's face template database").

As explained above, these allegations are false: Facebook does not create templates for non-users like Mr. Zellmer, nor does it retain the face signatures generated from images of non-users. *See* pp. 6-7 *supra*. No face template was created for Mr. Zellmer, and he has never been recognized or identified in content on Facebook through the use of face recognition. McCoy Decl. ¶ 15. Any face signature created from a photo of Mr. Zellmer that was uploaded to Facebook was useless for purposes of identification and was immediately discarded. *Id.* ¶ 16.

Mr. Zellmer purports to represent a class of "[a]ll individuals who have never subscribed to Facebook.com or any other Facebook, Inc. service and, while residing in Illinois, whose face was depicted in a photograph uploaded to Facebook.com from a device assigned an Illinois-based internet protocol address at any point in time between August 31, 2010 and the present." Compl. ¶ 42. He seeks statutory damages and injunctive relief "necessary to protect the interests of the class, including . . . an order requiring Facebook to collect, store, and use biometric identifiers or biometric information in compliance with the BIPA." *Id.* Prayer (C)-(D). At his deposition in this case, he recognized that this remedy would require Facebook to shut down facial recognition entirely, both as to users and non-users. Zellmer Dep. (Ex. 1) at 81, 119.

## SUMMARY JUDGMENT STANDARD

Summary judgment is warranted when "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). The moving party "bears the initial responsibility of . . . identifying those portions of [the record] which it believes demonstrate the absence of a genuine issue of material fact," *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986), either by "produc[ing] evidence negating an essential element of the nonmoving party's claim," or by "show[ing] that the nonmoving party does not have enough evidence of an essential element," *Nissan Fire & Marine Ins. Co. v. Fritz Cos.*, 210 F.3d 1099, 1102 (9th Cir. 2000). If the movant meets this initial burden, the burden then shifts to the non-movant to "produce evidence to support its claim or defense." *Id.* at 1103.

## ARGUMENT

BIPA is a notice-and-consent statute. But Mr. Zellmer wants to apply the statute to a class of people—Illinois non-users—who could not possibly be notified or give consent in advance of the challenged conduct. As this Court has explained, that is not "what the BIPA was supposed to address." Facebook should be granted summary judgment for each of three independent reasons. First, because data derived from images of non-users is not and cannot be used to identify anyone, Facebook has not obtained Mr. Zellmer's "biometric identifiers" or "biometric information" under BIPA. Second, because Facebook immediately deleted any face signature derived from photos of Mr. Zellmer, it was never in "possession" of any data even arguably regulated by BIPA and did not "collect, capture, . . . or otherwise obtain" it. Third, because it would be impossible for Facebook to notify, or obtain consent from, non-users who appear in photos uploaded to Facebook, any application of BIPA to Mr. Zellmer would violate Illinois' longstanding rule against reading statutes to require something that cannot be done. At minimum, the Court should dismiss Mr. Zellmer's claim for injunctive relief, because his theory of BIPA would require Facebook to disable facial recognition entirely.[6]

## I. ANY DATA DERIVED FROM PLAINTIFF'S PHOTOS DOES NOT QUALIFY AS A "BIOMETRIC IDENTIFIER" OR "BIOMETRIC INFORMATION" BECAUSE IT CANNOT BE USED TO IDENTIFY ANYONE.

### A. There Is No Genuine Dispute That Facebook Does Not And Cannot Use Facial-Recognition Technology To Identify Non-Users Like Mr. Zellmer.

Facebook does not and cannot use facial recognition to identify a non-user like Mr. Zellmer. *See* pp. 6-7 *supra*. Facebook does not create templates for non-users. So even when Facebook's software is run on a non-user photo and a face signature is generated, it cannot produce a successful match. No identification occurs at any step of the process.

The first two steps of Facebook's pipeline *never* identify anyone (user or non-user). The first step—face detection—simply determines whether *any* face appears in a photo. McCoy Decl. ¶ 3; Taigman Dep. at 126-27, 130-33, 137-40, 171; Yadan Dep. at 98-99, 117-18. In the second step—alignment—the system locates a set of fiducial points on the face simply to center, orient, and scale the detected face image. McCoy Decl. ¶ 5; Taigman Dep. at 150-53, 159-67, 177-78. The fiducial points help *warp* and *normalize* individual face geometry, not distinguish among faces. McCoy Decl. ¶ 5; Taigman Dep. at 366-67. They are not used to create face signatures, create templates, or otherwise attempt to determine someone's identity; the only information passed to the next step is the pixel array of the standardized image, not the fiducial points. McCoy Decl. ¶ 5; Taigman Dep. at 172.

In the third and fourth steps—representation and classification—Facebook attempts to identify *users* who have assented to facial recognition. When a user uploads a photo with a

[6] Facebook's position is that neither a face signature nor a template is a "scan of face geometry" within the meaning of BIPA, but it is not seeking summary judgment on that ground.

*non-user's* face, Facebook's software sometimes (but not always) calculates a *face signature* for that image and compares it to the templates of the uploader's friends. McCoy Decl. ¶¶ 7, 9. But because Facebook never creates *templates* for non-users (*id.* ¶ 13; McCoy Dep. at 39-40; Taigman Dep. at 369), a photo of a non-user like Mr. Zellmer will never generate a match, and the face signature will be discarded immediately (McCoy Decl. ¶¶ 8, 11, 16; McCoy Dep. at 154-55; Taigman Dep. at 368).

In short, Facebook has no way of identifying non-users like Mr. Zellmer in photos; Facebook does not retain identifying records of them and does not know who they are. Thus, as discussed next, any data derived from non-user photos is not regulated by BIPA.

## B. BIPA Regulates Only Data That Is Used For Identification.

### 1. The Text Of BIPA Covers Only Information That Can Be Used to Identify A Person.

BIPA regulates two sets of data: "biometric identifiers" and "biometric information." 740 ILCS 14/10 (emphasis added). As the Illinois Attorney General has explained, "the phrase 'biometric identifier' is commonly understood to refer to the measurement and analysis of a unique physical or behavioral characteristic *that identifies a person*." Ill. AG Op., 2017 WL 10084298, at *3 (emphasis added). Although BIPA defines a "*complete set* of *specific* qualifying biometric identifiers," including scans of face geometry, "[e]ach specific item on the list, not surprisingly, fits within the meaning of the term 'biometric identifier,' that is, a biology-based set of measurements ('biometric') that can be *used to identify a person* ('*identifier*')." *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017) (third emphasis added); *see also* WEBSTER'S DICTIONARY (2008 ed.) (EX. 7) (defining "identifier" as "one that identifies," and "identify" as "[t]o establish the identity of"); CAMBRIDGE DICTIONARY (2008 ed.) (Ex. 8) ("identify" means "to recognize or be able to name someone or something").

Similarly, BIPA defines "biometric information" as data "based on an individual's biometric identifier" that is "*used to identify* an individual." 740 ILCS 14/10 (emphasis added). As the *Rivera* court explained, this definition is designed to ensure that "whatever a private entity does in manipulating a biometric identifier into a piece of information, the resulting information is still covered by [BIPA] *if* that information can be *used to identify the person*." 238 F. Supp. 3d at 1095 (emphases added).

BIPA's legislative findings confirm the meaning of these terms. The statute describes the regulated data as "unique identifiers" that are "biologically unique to the individual" and can be "used to access finances or other sensitive information." 740 ILCS 14/5(c). The legislature was concerned that when a person's biometric data is "compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.* It is impossible to commit "identity theft" using data that is incapable of identifying anyone.

BIPA's regulating provisions point in the same direction. In addition to regulating entities that "possess[]" (*id.* 14/15(a)) and "collect" (*id.* 14/15(b)) biometric data, the statute requires private entities to protect biometric data in a manner consistent with the way they protect "*other* confidential and sensitive information" (*id.* 14/15(e)(2) (emphasis added)). The statute defines "confidential and sensitive information" as "personal information that can be used to *uniquely identify an individual* or an individual's account or property." *Id.* 14/10 (emphases added)).

In short, BIPA regulates data used for identification. And there is no genuine dispute that Facebook cannot use Mr. Zellmer's face signature to "uniquely identify an individual." *Id.*

### 2. The Cases Confirm This Point.

Several courts have confirmed that BIPA is designed to regulate only data that can be used for identification, including the Ninth Circuit in *Facebook Biometric*. There, the court held that the user plaintiffs had adequately alleged an injury in fact for purposes of Article III standing. *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1270-75 (9th Cir. 2019). In doing so, it relied on the user plaintiffs' allegation that Facebook had created templates for them that could be associated with their user profiles and used to identify them in subsequent images uploaded to Facebook: "Once a face template of an individual is created [from a photo], Facebook can use it to identify that individual in any of the other hundreds of millions of photos uploaded to Facebook each day, as well as determine when the individual was present at a specific location." *Id.* at 1273. The court found that the "substantive harm targeted by BIPA" is "Facebook's alleged collection, use, and storage of plaintiffs' *face templates*." *Id.* at 1275 (emphasis added); *see id.* at 1269 (describing General Assembly's finding that "'[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information,' because while social security numbers can be changed if compromised by hackers, biometric data are 'biologically unique to the individual,' and 'once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions'" (quoting 740 ILCS 14/5(c))).

Other decisions are in accord, including this Court's decision in *Gullen*. *See* 2018 WL 1609337, at *2 (noting that "some photos uploaded to Facebook are not analyzed for *user matches*" (emphasis added)); *Mutnick v. Clearview AI, Inc.*, 2020 WL 4676667, at *1-2 (N.D. Ill. Aug. 12, 2020) (finding that "plaintiffs' privacy rights were violated" where "defendants built a searchable database of the scanned images enabling database users to instantly identify unknown individuals using nothing more than a photograph"); *Monroy v. Shutterfly, Inc.*, 2017 WL 4099846, at *1 (N.D. Ill. Sept. 15, 2017) (finding that someone "can be *uniquely identified* by his face geometry in the same way that he can be identified by his fingerprints" (emphasis added)).

One court has taken a narrower view of BIPA's identification requirement, but even this view of BIPA would not permit Mr. Zellmer's claim to survive summary judgment. In *Hazlitt v. Apple, Inc.*, 2020 WL 6681374 (S.D. Ill. Nov. 12, 2020), the plaintiffs challenged an Apple Photos feature that groups pictures with the same face. The plaintiffs alleged that Apple "store[d]" the data generated by this feature "on each Apple device locally in a facial recognition database," and that "Apple [did] not delete the biometric data it collect[ed] on the devices, even discarded Apple devices." *Id.* at *2. They further alleged that "because this information is stored on individual devices, Plaintiffs . . . face[d] the imminent threat of disclosure of their biometric data as a result of a data breach on any Apple device on which their biometric data [was] stored." *Id.*

Apple moved to dismiss, arguing that "the purported facial templates" identified in the complaint did "not qualify as biometric identifiers as defined by BIPA because they are anonymous and do not actually identify any individual." *Id.* at *7. The court disagreed, finding that "[t]he word 'identifier' modifies the word 'biometric' to signal that the types of data listed *could* be used to identify a person." *Id.* at *8. The court also noted that the plaintiffs had alleged that Apple *did* use the technology to identify people in photos, and that this allegation had to be "[t]aken as true[] at [the pleading] stage." *Id.*

*Hazlitt* is distinguishable for several reasons. First, it is undisputed that when Facebook creates a face signature for a non-user like Mr. Zellmer, that signature *cannot* be used for identification. *See* pp. 6-7 *supra*. Second, because the data was immediately deleted, there is *no* "threat of disclosure of [Mr. Zellmer's] biometric data as a result of a data breach," much less an "imminent threat." *Hazlitt*, 2020 WL 6681374, at *2. Third, because this case is at the summary judgment stage, the Court need not accept Mr. Zellmer's allegation that Facebook creates "purported templates" (*id.* at *7) from the images of non-users like him; that claim has been refuted by discovery. *See* pp. 6-7 *supra*.

In any event, *Hazlitt* was wrongly decided. A biometric identifier is "a unique physical or behavior characteristic *that identifies a person*." Ill. AG Op., 2017 WL 10084298, at *3 (emphasis added). And "biometric information" encompasses only data that *is* "used to identify an individual." 740 ILCS 14/10. When an entity does not and cannot use data to identify someone and deliberately deletes it upon finding that it does not match a registered, consenting user, it has not collected "biometric identifiers" or "biometric information" under the only sensible reading of those terms and the statute's legislative history.

## II. FACEBOOK WAS NEVER IN "POSSESSION" OF MR. ZELLMER'S ALLEGED "SCAN OF FACE GEOMETRY" AND DID NOT "COLLECT," "CAPTURE," "OR OTHERWISE OBTAIN" IT.

### A. Facebook Did Not Create A Template For Mr. Zellmer Or Retain A Face Signature For Him.

As discussed above (*see* pp. 6-7 *supra*), there is no genuine dispute that Facebook does not create, save, or store templates for non-users who appear in photos, and that Mr. Zellmer has never had a template. McCoy Decl. ¶ 13; McCoy Dep. at 39-40; Taigman Dep. at 369. When a face signature is created from an image of a non-user like Mr. Zellmer, it is immediately discarded. McCoy Decl. ¶¶ 8, 11, 16; McCoy Dep. at 40-41; Taigman Dep. at 368. And this data is useless outside Facebook's specific network. McCoy Decl. ¶¶ 11-12.

### B. BIPA Regulates Only Data That Is Retained And Controlled.

#### 1. The Text Of BIPA Is Limited To Retained Data.

BIPA's notice-and-consent requirements apply only to private entities "in possession of biometric identifiers or biometric information" (740 ILCS 14/15(a)) and those that "collect, capture, purchase, receive through trade, or otherwise obtain a person's or customer's biometric identifiers or biometric information" (*id.* 14/15(b)). Each term connotes at least *temporary retention* of, and *control* over, the data. "Possess" is commonly defined as "to seize and take control of"; "collect" means "to gain or regain control of"; "capture" is defined as "gaining control"; and "obtain" means "to gain or attain." *See* MERRIAM-WEBSTER.COM DICTIONARY, *available at* https://www.merriam-webster.com/dictionary (last visited May 17, 2021); *see also* BLACK'S LAW DICTIONARY (defining "obtain" as "[t]o bring into one's own possession"). None of these terms can reasonably apply to data that is discarded immediately upon creation.[7]

The legislative findings point in the same direction: The mere creation of data, without subsequent possession or control of it, does not raise any "heightened risk for identity theft." 740 ILCS 14/5(c). Such data cannot be "compromised." *Id.* Nor can it be "tied to finances and other personal information." *Id.* 14/5(d). There is no risk that *Facebook* will use Mr. Zellmer's face signature, much less that a third party will be able to hack or misuse it. *Cf. Patel,* 932 F.3d at 1273 ("The judgment of the Illinois General Assembly . . . supports the conclusion that the *capture and use* of a person's biometric invades concreate interests." (emphasis added)).

#### 2. The Cases Confirm This Point.

Several district courts in Illinois have interpreted the text of Section 15 of BIPA. These decisions confirm Facebook's reading of that provision.

The first such case was *Namuwonge v. Kronos, Inc.*, 418 F. Supp. 3d 279 (N.D. Ill. 2019). The defendant, Kronos, made "devices that enable employers to process payroll and track employee time." *Id.* at 281-82. It sold those devices to third-party Brookdale, an operator of senior

[7] To the extent any of BIPA's terms is broader than the others, it must be "narrowed by . . . the neighboring words with which it is associated," *United States v. Williams*, 553 U.S. 285, 294 (2008), "to avoid ascribing to one [term] a meaning so broad that it is inconsistent with its accompanying words," *People v. Qualls*, 365 Ill. App. 3d 1015, 1020 (2006).

living communities. *Id.* The plaintiff, an employee of Brookdale, claimed that Brookdale used a Kronos device to collect and store his fingerprint data, and that Kronos violated BIPA by failing to give him notice or obtain his consent before his data was generated. *Id.* He also claimed that Brookdale disclosed his fingerprint data to Kronos. *Id.* Kronos moved to dismiss. *Id.* at 281.

The court granted the motion in part and denied it in part. *Id.* It first addressed whether the plaintiff "adequately pleaded that Kronos actually possessed Brookdale employees' biometric data as required under [Section] 15(a)." *Id.* at 283. The court explained that under Illinois Supreme Court precedent, "possession 'occurs when a person *has or takes control* of the subject property or *holds the property at his or her disposal*.'" *Id.* (emphases added) (quoting *People v. Ward*, 215 Ill. 2d 317, 325 (2005)). The court held that the plaintiff's "allegation that Brookdale disclosed their employees' fingerprint data to Kronos"—which Kronos kept—was sufficient to satisfy that definition. *Id.* at 284. The court held, however, that the plaintiff had failed to adequately allege a violation of Section 15(b) of BIPA, because the terms "collect, capture, . . . or otherwise obtain" require that the data be obtained directly from the plaintiff, whereas Brookdale was the party that had "collected the fingerprints using a system that Kronos supplied to Brookdale." *Id.* at 286.

To be sure, *Namuwonge* was decided in a different context from this case: there was a third-party intermediary between the defendant and the plaintiff, whereas here Facebook is the only alleged possessor and collector of Mr. Zellmer's biometric data. But a similar principle applies. Facebook does not "hold [Mr. Zellmer's] data at [Facebook's] disposal." *Ward*, 215 Ill. 2d at 325. And it has avoided taking "control" over that data through the design of its facial-recognition technology.

A more recent BIPA case, *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960 (N.D. Ill. 2020), further confirms that Section 15 requires at least temporary retention of biometric data. Like *Namuwonge*, *Heard* involved a defendant (Becton Dickinson, which the court referred to as "BD") that sold fingerprinting devices to the plaintiff's third-party employers (five hospitals). *Id.* at 962. Unlike in *Namuwonge*, however, the plaintiff did *not* explain how the defendant (as distinct from the hospitals) received his fingerprint data. *See id.* at 967. The court held that the plaintiff had not "plausibly alleged that BD 'collect[ed], captur[ed], purchase[d], receive[d] through trade, or otherwise obtain[ed]' [the plaintiff's] biometric data," because his complaint did not explain "*how the data made its way to BD's systems*." *Id.* (emphasis added). The court then held that the plaintiff had not even "adequately pleaded 'possession' because he fail[ed] to allege that [the defendant] exercised *any dominion or control over his biometric data*." *Id.* at 968 (emphasis added) (quotation marks and alteration omitted). The plaintiff did "not say whether [the defendant] could *freely access* the data" or "held the data at its disposal." *Id.* (emphasis added).

Here, the evidence is undisputed that Facebook *cannot* "freely access" Mr. Zellmer's face signature—because its system is deliberately constructed to discard this data upon creation. Facebook has not obtained or possessed his "biometric identifier" or "biometric information."

## III. BIPA DOES NOT REQUIRE IMPOSSIBLE NOTICE AND CONSENT.

Mr. Zellmer cannot satisfy the elements of BIPA. But there is a more fundamental problem with his claim: As detailed above (at 6-7), there is no feasible way for Facebook to give notice to, or obtain consent from, non-users who appear in photos uploaded to Facebook. Mr. Zellmer therefore seeks a reading of BIPA that would require Facebook to disable the technology; he admitted as much at his deposition. Zellmer Dep. at 81, 119. Indeed, his reading would make it impossible to use biometric systems for *any* security purpose—the very application the legislature had in mind. As this Court recognized in *Gullen*, the statute should not be read that way.

Under Illinois law, a court must "presume that the General Assembly, in its enactment of legislation, did not intend absurdity, inconvenience or injustice." *Chatham Foot Specialists, P.C. v. Health Care Serv. Corp.*, 216 Ill. 2d 366, 382 (2005); *see also Solon v. Midw. Med. Records Ass'n, Inc.*, 236 Ill. 2d 433, 441 (2010) ("We may [ ] consider the consequences that would result from construing the statute one way or the other. In doing so, we presume that the legislature did not intend absurd, inconvenient, or unjust consequences." (citation omitted)). Applying this principle, Illinois courts have routinely refused to read statutes in a way that would make compliance impossible. *See, e.g.*, *McDonald v. City of Spring Valley*, 285 Ill. 52, 56 (1918) ("It would be unreasonable to [ ] construe [a] statute as to make it appear that the Legislature intended . . . to require that to be done which is utterly impossible of performance."); *People v. Russell*, 2012 IL App (2d) 111098-U, ¶ 15 (2012) ("[O]ur task is to effectuate the obvious intent of the

General Assembly . . . while avoiding the absurd result of punishing [defendants] where literal compliance with [the statute] is impossible.").

BIPA should be no exception. The statute was intended to *regulate* the collection and storage of biometric data, not to preclude it. The General Assembly found that "[t]he use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings." 740 ILCS 14/5(a). It was optimistic about the fact that "[m]ajor national corporations ha[d] selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." *Id.* 14/5(b). And the legislature was worried that "many members of the public [were being] *deterred from partaking* in biometric identifier-facilitated transactions." *Id.* 14/5(e) (emphasis added). In other words, the goal was to *promote* the use of biometric technologies through reasonable notice-and-consent measures, not to ban them entirely.

The Illinois Supreme Court's only decision construing BIPA, *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186 (2019), further supports this point. There, the court held that "an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under [BIPA], in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act." *Id.* ¶ 40. The court found that BIPA was intended to give private entities "the strongest possible incentives to *conform to the law* and prevent problems before they occur," particularly because "*[c]ompliance should not be difficult.*" *Id.* ¶ 37 (emphases added). Thus, the legislature "vest[ed] in individuals and customers the right to control their biometric information by requiring notice before collection and giving them the power to say no by withholding consent." *Id.* ¶ 34. Nothing in BIPA or *Rosenbach* suggests that the legislature wanted to ban certain technologies.

If BIPA were applied to an entity's creation of ephemeral data, like face signatures, it would ban more than just Facebook's technology; many prevalent applications of biometric technology would be infeasible. For example, consider a company that obtains consent from its employees before implementing a biometric security system that controls access to sensitive areas of an industrial plant. Under Mr. Zellmer's reading of the statute, the company would be liable under BIPA to a would-be *intruder* for analyzing his face and running the result against the faces of authorized entrants before finding no match, denying the intruder entry, deleting his data, and sounding an alarm. The whole purpose of a biometric security system is to flag individuals that the system *cannot* recognize—and who necessarily have not given "consent" to the entity's use of biometrics. That is not the purpose of *Facebook's* facial-recognition system, but the process—generate a face signature, run it against a set of consenting users, and then immediately discard it if there is no match—works the same way as many automated security systems.

The Court was correct in *Gullen*: It would be "patently unreasonable" to interpret "a written consent statute" in a way that would amount to a "ban [o]n the program." Ex. 5 at 9-10. That is "more than Illinois contemplated." Ex. 6 at 31-34. Mr. Gullen's counsel never explained "how a . . . written notification and consent statute can apply to people who are non-users." Ex. 5 at 9. Apart from a ban on facial recognition, the only proposal counsel made was for Facebook to get consent from *users* who uploaded photographs from Illinois. Ex. 6 at 31-33. But obtaining consent from the uploading users would not solve the alleged problem: that Facebook is failing to obtain consent from Illinois non-users like Mr. Zellmer who are *depicted* in the photos. BIPA requires a "written release executed by the subject of the biometric identifier" or his "legally authorized representative" (740 ILCS 14/15(b)), not by a stranger who posts a photo on Facebook.

In short, it would be impossible for Facebook to provide written notice to, or obtain consent from, non-users who merely appear in photos. By precluding Facebook and other entities from offering useful features that apply facial recognition to consenting users, Mr. Zellmer's interpretation of BIPA would adversely affect millions of people, all around the country, who are not in his proposed class. The Court was right that photos of non-users are not "what the BIPA was supposed to address." Facebook should be granted summary judgment.

## IV. PLAINTIFF CANNOT OBTAIN AN INJUNCTION.

If the Court does not grant summary judgment on the merits of Mr. Zellmer's claims, it should at minimum dismiss his claim for injunctive relief.

First, "the basis for injunctive relief . . . has always been irreparable injury and the inadequacy of legal remedies." *Weinberger v. Romero-Barcelo*, 456 U.S. 305, 312 (1982). Mr. Zellmer has not attempted to show any injury beyond the alleged violation of BIPA, let alone one that is irreparable and not "adequately compensable by money damages." *United Steel v. Shell Oil Co.*, 2010 WL 11508796, at *7 (C.D. Cal. Aug. 27, 2010). He has not raised a genuine dispute of fact that would allow him to proceed to trial on his claim for injunctive relief.

Second, injunctive relief is improper if "it isn't clear that all members of the class" would benefit from it. *Schulken v. Wash. Mut. Bank*, 2012 WL 28099, at *6 (N.D. Cal. Jan. 5, 2012). In light of Mr. Zellmer's proposed outright ban, that is an understatement. Given that Facebook stores no facial-recognition data about non-users, there is no reason to believe that *all* non-users have any qualms with the technology. And the proposed injunction would affect people who are not situated like Mr. Zellmer—most notably, people who *use* Facebook. Mr. Zellmer's proposal would therefore have an effect on a huge population of people who are not in his proposed class; have not sought an injunction; and will have no opportunity to object to it. That is improper. *See Stokes v. CitiMortgage, Inc.*, 2015 WL 709201, at *10 (C.D. Cal. Jan. 16, 2015) ("[T]he Court cannot order the injunctive relief Plaintiffs claim to seek. . . . [It] would necessarily affect Defendant's practices with regard to individuals who are not members of the putative class.").

## CONCLUSION

The Court should grant summary judgment in favor of Facebook on all of plaintiff's claims. In the alternative, it should grant summary judgment on his claim for injunctive relief.

Dated: May 17, 2021

MAYER BROWN LLP

By: /s/ *Lauren R. Goldman*
Lauren R. Goldman (*pro hac vice*)
Michael Rayfield (*pro hac vice*)
1221 Avenue of the Americas
New York, NY 10016
(212) 506-2500
lrgoldman@mayerbrown.com
mrayfield@mayerbrown.com

Matthew D. Provance (*pro hac vice*)
71 Wacker Drive
Chicago, IL 60606
(312) 701-8598
mprovance@mayerbrown.com

COOLEY LLP

Michael G. Rhodes (116127)
Whitty Somvichian (194463)
101 California Street, 5th Floor
San Francisco, CA 94111
(415) 693-2000
rhodesmg@cooley.com
wsomvichian@cooley.com

*Attorneys for Defendant Facebook, Inc.*